

A message from Sun Life:

Learn more about phishing emails

What are phishing emails?

Phishing emails are emails sent by cyber criminals, designed to get recipients to click on links or attachments that will spread malware (i.e. computer viruses). Cyber criminals are experts at manipulating recipients by preying on their desire to be helpful and respond quickly to requests.

How can you identify phishing emails?

Before you click on a link/attachment or reply to the email, here are some signs that you may have received a phishing email:

- The request you've been asked to review and respond to is from a person or organization you don't have a relationship with
- There are multiple spelling and grammar mistakes within the email
- Links/attachments appear suspicious when you hover your mouse over them
- You don't recognize the email address it was sent from

How can you determine if an email from Sun Life is legitimate?

If the email came from one of the following email addresses, it's from Sun Life:

- info@members-sunlife.com
- Sun_Life_Financial@email.sunlife.com
- CustomerCareCentre@sunlife.com
- @messages.sunlife.com
- @info.sunlife.com

From time to time, Sun Life engages external groups to send out legitimate email surveys to plan members. Review the section above to help you identify if these are legitimate or not.

What should you do if you receive or think you've received a phishing email regarding your pension account?

Never reply to or forward a phishing email, or click any of the links or attachments. If you're unsure if the email came from Sun Life, call us at **1-866-733-8612** any business day from 8 a.m. to 8 p.m. ET and we'll verify the email.

